DATE(S) ISSUED:

06/15/2011

SUBJECT:

Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS11-045)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Office Excel, a spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. The file may be received as an email attachment, or downloaded via the web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

·   Microsoft Office XP

·   Microsoft Office 2003

·   Microsoft Office 2007

·   Microsoft Office 2010

·   Microsoft Office 2004 for Mac

·   Microsoft Office 2008 for Mac

·   Microsoft Office for Mac 2011

·   Open XML File Format Converter for Mac

·   Microsoft Excel Viewer

·   Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats

RISK:

Government:
·   Large and medium government entities: **High**
·   Small government entities: **High**

Businesses:
·   Large and medium business entities: **High**
·   Small business entities: **High**

Home users:High

DESCRIPTION:

Eight vulnerabilities have been privately reported in Microsoft Excel. These vulnerabilities can be triggered by opening a specially crafted Excel file and can be exploited via email or through the web. In the email-based scenario, the user would have to open the specially crafted Excel file as an email attachment. In the web based scenario, a user would have to open the specially crafted Excel file that is hosted on a website. When the user opens the Excel file, the attacker's supplied code will execute. Details of these vulnerabilities are as follows:

Record Parsing Vulnerabilities

Two remote code execution vulnerabilities exist in the way Excel parses and validates records in Excel files.

Memory Corruption Vulnerabilities

Six remote code execution vulnerabilities exist in the way Excel accesses objects in memory that have not been properly initialized or deleted.

Successful exploitation could result in an attacker gaining the same privileges as thelogged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:
·   Apply appropriate patches provided by Microsoft to vulnerable systems immediatelyafter appropriate testing.
·   Consider installing Microsoft's Office File Validation tool for Microsoft Excel 2003 and Excel 2007 (http://www.microsoft.com/technet/security/advisory/2501584.mspx) which would prompt the user for files that fail the Office File Validation and a user would have to click through the warning messages to open them before any of these vulnerabilities are exploited.
·   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
·   Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-045.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1272

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1273

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1274

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1275

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1276

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1277

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1278

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1279

SecurityFocus:

http://www.securityfocus.com/bid/48157

http://www.securityfocus.com/bid/48158

http://www.securityfocus.com/bid/48159

http://www.securityfocus.com/bid/48160

http://www.securityfocus.com/bid/48161

http://www.securityfocus.com/bid/48162

http://www.securityfocus.com/bid/48163

http://www.securityfocus.com/bid/48164